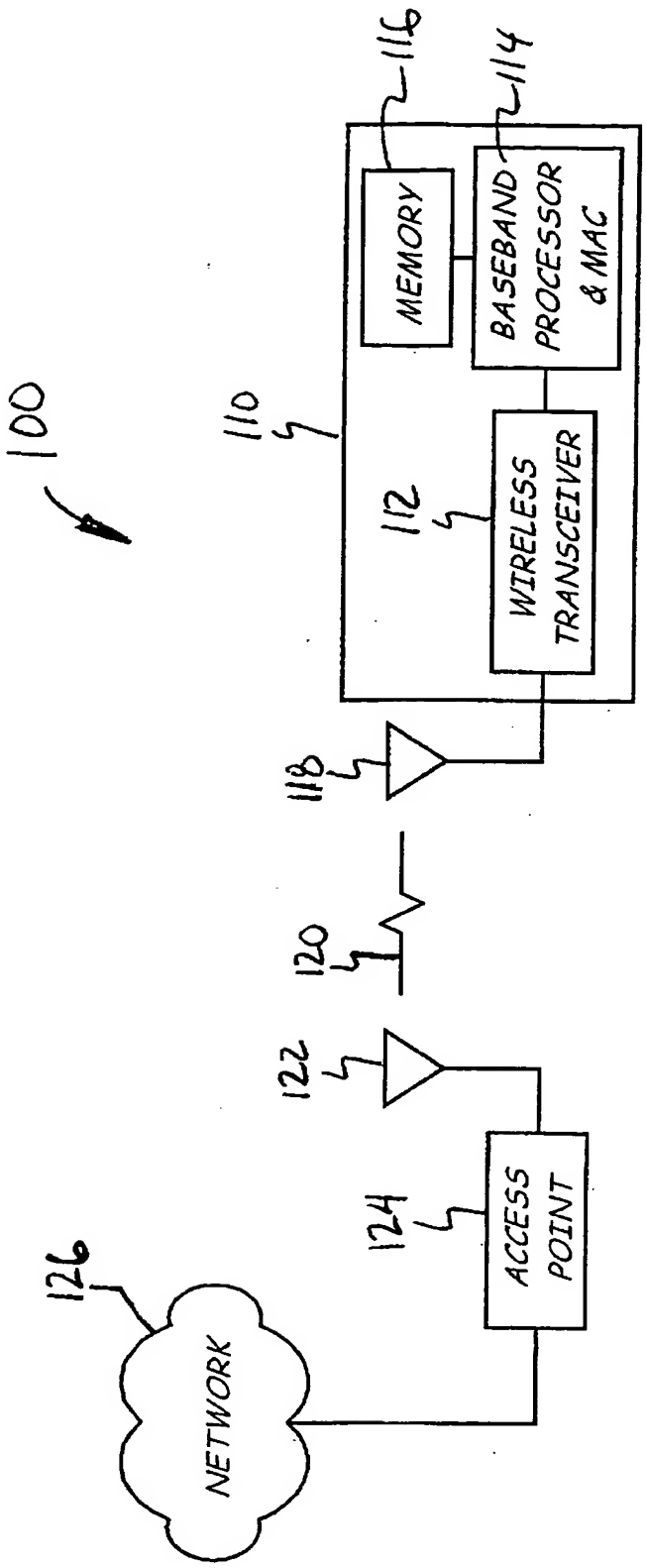
100
110
112
116
114
MEMORY
BASEBAND PROCESSOR & MAC
WIRELESS TRANSCEIVER
118
120
122
124
ACCESS POINT
126
NETWORK

FIG. 1

COMMUNICATION	INFORMATION TRANSFERRED
AP → STA (PROBE RESPONSE)	ANONCE
STA → AP (REASSOCIATE REQUEST)	ANONCE, SNONCE, MIC1
AP → STA (REASSOCIATE RESPONSE)	SNONCE, MIC2

FIG. 2

300

Element ID	Length	Nonce
1 octet	1 octet	32 octets

FIG. 3

400

Element ID	Length	Key ID	ANonce	SNonce	MIC
1 octet	1 octet	8 octets	32 Octets	32 Octets	16 octets

FIG 4

500

Element ID	Length	Key ID	GTK Length	Wrapped GTK	RSC	GNonce	MIC
1 octet	1 octet	8 octets	1 octet	GTK length octets	6 Octets	32 Octets	16 octets

FIG. 5

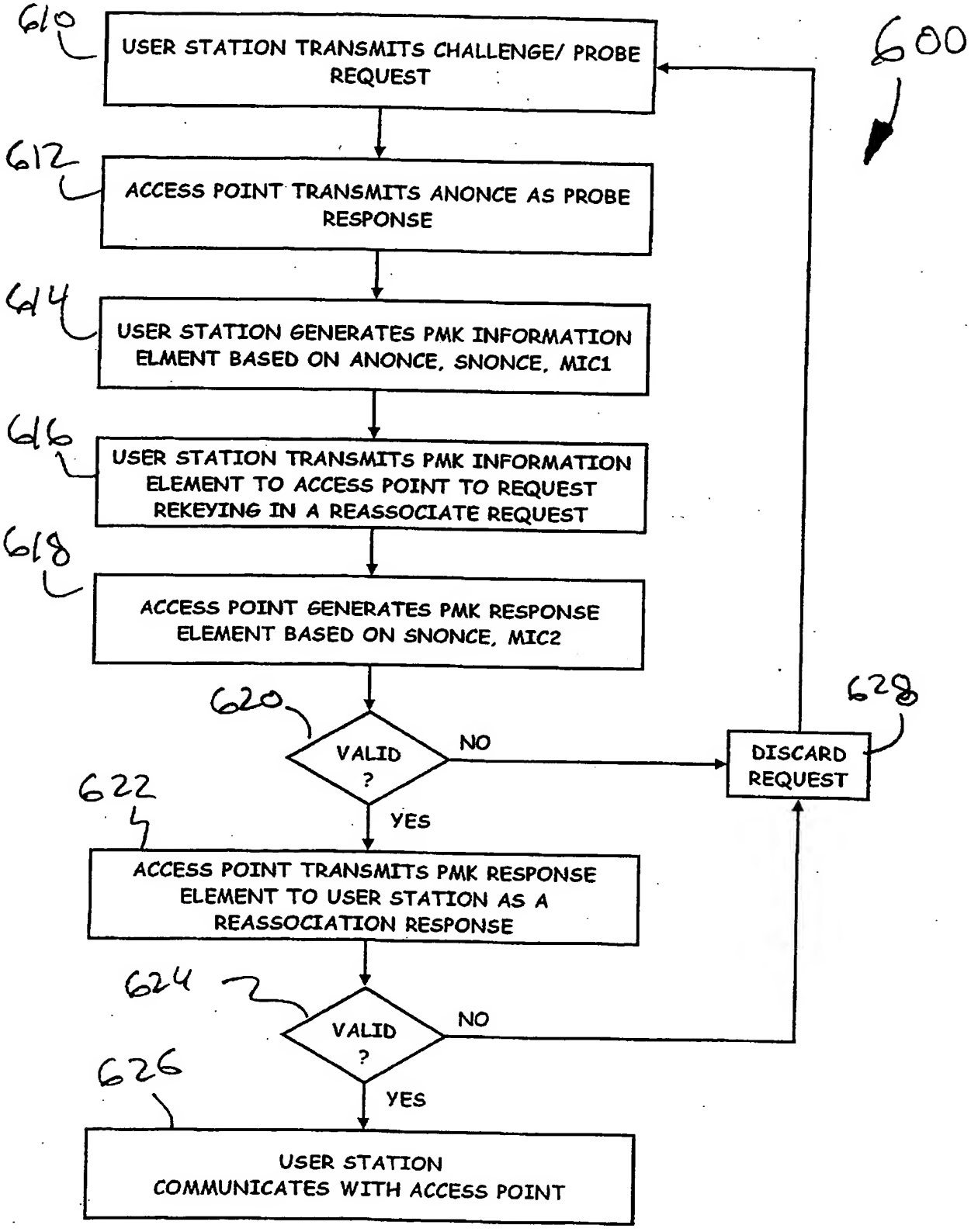
600
610
USER STATION TRANSMITS CHALLENGE/ PROBE REQUEST
612
ACCESS POINT TRANSMITS ANONCE AS PROBE RESPONSE
614
USER STATION GENERATES PMK INFORMATION ELMENT BASED ON ANONCE, SNONCE, MIC1
616
USER STATION TRANSMITS PMK INFORMATION ELEMENT TO ACCESS POINT TO REQUEST REKEYING IN A REASSOCIATE REQUEST
618
ACCESS POINT GENERATES PMK RESPONSE ELEMENT BASED ON SNONCE, MIC2
620
VALID ?
NO
628
DISCARD REQUEST
YES
622
ACCESS POINT TRANSMITS PMK RESPONSE ELEMENT TO USER STATION AS A REASSOCIATION RESPONSE
624
VALID ?
NO
YES
626
USER STATION COMMUNICATES WITH ACCESS POINT

FIG. 6